

anm^o



Building Blocks for a Cyber-Resilient Infrastructure

CONTENTS

- 01 Cyber Resilience Defined
- 02 4 Pillars of Cyber Resilience
- 03 The Cyber Resilience Foundation
- 04 Data Protection
- 05 Disaster Recovery
- 06 Incident Response
- 07 Conclusion



01

Cyber Resilience Defined

The inevitability of encountering a cyber-related incident for organizations is not a question of if but when. Whether it be a cyberattack, system failure, natural disaster, or a simple human error, the unpredictable nature of these events highlights the necessity for cyber resilience as a defense mechanism to keeping your organization safe.

So, what is cyber resilience? [NIST SP 800-172](#) defines cyber resiliency as “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.”

Simply put, cyber resilience marries cybersecurity and business continuity to create an environment where both disciplines work together to maximize effectiveness and protect the organization from cyberthreats.

But why now is this term rising to the top of so many cyber-risk conversations?

Because, as ANM security expert Matthew Martinez states, “We need a different approach, not just to defend ourselves from cyberattacks and failures, but to presume that attacks will always get through and are unavoidable. We need to be resilient in the face of attacks and failures so we can withstand or recover quickly. We need a fundamental re-imagining based on taking a holistic, systems-thinking approach.”

In this eBook, we explore what this re-imagining entails, from the four essential pillars in cyber resilience, the required foundation and how data protection, disaster recovery and incident response must work together for true cyber resilience.

The average ransomware payout has increased dramatically from **\$812,380** in 2022 to **\$1,542,333** in 2023.

- [SC Magazine](#)



02

4 Pillars of Cyber Resilience

Cyber-resilient systems have security measures or safeguards “built in” as a foundational part of the architecture and design, not unlike the human body.

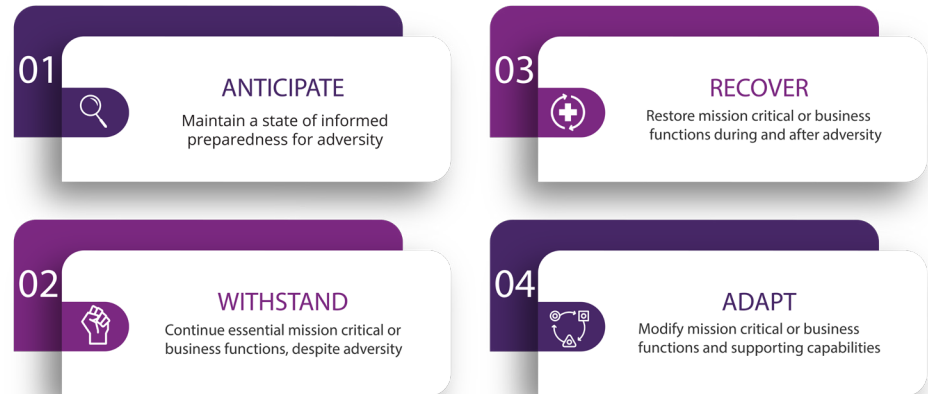
The human body has an immune system that can readily absorb a continuous barrage of environmental hazards and provides the necessary defense mechanisms to maintain a healthy state. Additionally, the body has self-repair systems to recover from illnesses and injuries when defenses are breached.

But cyber-resilient systems, like the human body, cannot defend against all hazards at all times. While the body cannot always recover to the same state as before an injury or illness, it can adapt. Similarly, cyber-resilient systems can recover minimal essential functionality to meet critical mission needs.

Just like understanding the limitations of individuals, understanding the limitation of organizations and systems is fundamental to managing risk and can be broken down into these four key pillars.

1. **Anticipate:** This goal is to maintain a state of informed preparedness for adversity. This involves identifying and mitigating weaknesses, but also contingency planning for threat events to ensure you can investigate and respond to the discovery of vulnerabilities or compromises.
2. **Withstand:** This goal is to continue your essential mission or business functions, despite adversity. Naturally, this requires identifying your essential mission and business functions, along with all supporting processes, systems, services and infrastructures. It’s important to remember that the criticality of functions and their supporting capabilities can change over time.

3. **Recover:** The third goal is to restore your mission critical or business functions during and after adversity, possibly using a staged (incremental) process. It’s vital to ensure that recovery does not restore the threat; for example, restoring a system from backup without sufficient precautions might also restore a backdoor that an adversary planted weeks ago.
4. **Adapt:** The final goal is to modify your mission or business functions and their supporting capabilities in response to changes in your IT environment and the threat landscape.



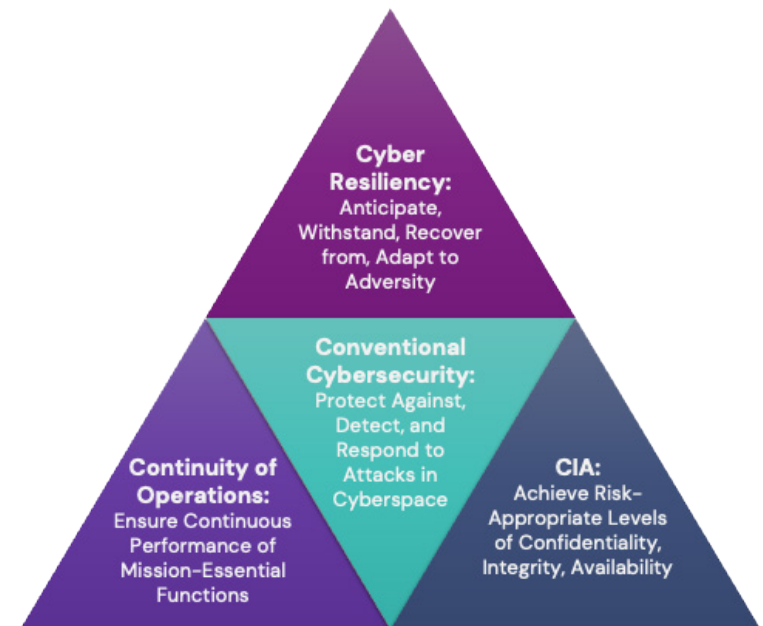
03

The Cyber Resilience Foundation

Formal cyber-resilience frameworks are architectural approaches to achieving or improving resilience in the face of cyber threats. Therefore, objectives and techniques that relate to organizational resilience or business continuity in the face of non-cyber threats (e.g., natural disaster, human error, system failures) are not included directly as part of those frameworks. The NIST and MITRE Frameworks assume a good foundation of conventional security, cybersecurity, and Continuity of Operations (COOP) policies, procedures, technologies and practices.

In the journey towards achieving cyber resilience, establishing robust foundational capabilities is pivotal. These key strategies form the bedrock of an effective cyber-resilient framework.

- **Authentication - Protecting Against User Compromise:** Authentication is the first line of defense against unauthorized access. Consider separating authentication domains for the Control Plane (CP) and Workloads (WL) to enhance security. Implement Multi-factor Authentication (MFA) and adhere to the principle of least privilege to restrict access rights. Robust auditing mechanisms for login failures and user changes provide critical insights into potential security threats.
- **Network Isolation of Control Plane:** Network isolation is a fundamental strategy for safeguarding the Control Plane (CP). Utilize separate VLANs with firewall (FW) inspection, following best practices from VMware and other relevant vendors. Employ Next-Generation Firewalls (NGFWs) with meticulous inbound and outbound rules, and leverage jump boxes to control and monitor access to critical infrastructure.
- **Vulnerability/Lifecycle Management & Patching:** Prioritize vulnerability and lifecycle management to stay ahead of potential threats. Regularly patch all CP devices to address known vulnerabilities and bolster the security posture of your infrastructure.
- **Modern Endpoint Protection:** Extend endpoint protection measures to both the CP and workloads. Implementing advanced solutions shields devices from a multitude of threats, providing an additional layer of defense against evolving cyber risks.





87% of organizations have a risk management program that drives their security roadmap or strategy. That said, only 35% believe their program is working well, while 52% are seeking to improve their situation and the remaining 13% do not yet even have an established program.

- Veeam

- **Logging & Auditing:** Comprehensive logging and auditing are integral components of cyber resilience. Establish robust mechanisms for monitoring, logging, and auditing activities. Implement alerting systems to promptly respond to anomalies, ensuring a proactive approach to potential security incidents.
- **Monitoring:** Continuous monitoring of network activities, user behaviors, and system performance is imperative. Utilize advanced monitoring tools to detect anomalies, identify potential threats, and respond swiftly to security incidents.
- **Redundancy & High Availability:** To fortify cyber resilience, eliminate single points of failure by building redundancy into your infrastructure. Ensure high availability across critical components, reducing the impact of system failures and enhancing overall resilience.

Incorporating these strategies into your cyber resilience framework establishes a solid foundation, enabling your organization to navigate the ever-evolving threat landscape with confidence. By adopting a proactive and holistic approach to security, you not only mitigate risks but also position your organization to recover swiftly from potential cyber incidents.

04

Data Protection

Backups are worthless if data can't be restored when needed, and with confidence that the restored data is accurate, complete, and free of malware. To ensure this scenario is avoided, you need an effective data protection strategy with:

- Backup and retention
- Restoration
- Visibility and analytics

Backup & Retention

To safeguard invaluable data, a robust backup and retention strategy is critical. This includes:

- **Documented Strategy & Policy:** An effective backup and retention strategy begins with a meticulously documented policy. This policy should outline the organization's approach to data protection, establishing the foundation for subsequent decisions and actions. The documentation should cover the types of data considered critical, the frequency of backups, the retention period, and the procedures for recovery.
- **3-2-1 Rule:** At the core of any effective backup strategy lies the 3-2-1 rule. This rule dictates that organizations should maintain three copies of their data: the original data and two backups. These backups should be stored on two different media types, with one copy stored offsite. This redundancy ensures data availability even in the face of localized disasters or hardware failures.
- **Snapshots, Backups, Archives:** Understanding the nuances of snapshots, backups, and archives is pivotal in designing a resilient data protection strategy. Snapshots offer point-in-time copies of data, allowing for quick recovery in case of accidental deletions or corruptions. Backups provide a more comprehensive copy of the data, often stored in a different location or medium. Archives, on the other hand, are long-term storage solutions, typically reserved for regulatory compliance or historical purposes.
- **On-prem, Cloud, SaaS:** Organizations have many options when it comes to implementing their backup and retention strategy. On-premises solutions offer complete control and customization but require significant infrastructure investments. Cloud-based solutions provide scalability and accessibility but necessitate a reliable internet connection. SaaS offerings, meanwhile, delegate data protection responsibilities to service providers, freeing organizations from infrastructure management.
- **Secure "Immutable" Copies:** In an era of evolving cyber threats, ensuring the security of backups is paramount. Creating immutable copies, or copies that cannot be altered or deleted, safeguards against ransomware attacks and unauthorized access. Implementing security measures such as encryption and access controls further fortifies the resilience of the backup infrastructure.
- **Service Level Objectives (SLOs):** SLOs define the acceptable parameters for data protection. Two critical elements of SLOs are the Recovery Point Objective (RPO), indicating the maximum allowable data loss in case of an incident, and Retention, specifying the duration backups are retained.
- **System & Data Inventory:** An often overlooked but crucial aspect of an effective backup strategy is maintaining a comprehensive system and data inventory. Understanding the organization's data landscape facilitates informed decisions regarding what to back up, how frequently to do so, and where to store the backups.

Restoration

A well-defined backup strategy is only as good as its restore process, and an effective restore process has these crucial elements:

- **Documented Restore Process:** A documented restore process serves as the roadmap to recovery. This comprehensive document outlines step-by-step procedures for retrieving data from backups, specifying roles and responsibilities, and ensuring a systematic approach to restoration. It acts as a crucial resource during high-stress situations, guiding IT professionals through the intricacies of data recovery.
- **Ease of Finding Specific Data to Restore:** The efficiency of a restore process is heavily reliant on how easily specific data can be identified and retrieved. Well-organized backups with clear naming conventions and categorization significantly contribute to the ease of locating the required data. Tools and interfaces that facilitate quick searches and intuitive navigation further streamline the restoration process.
- **Speed of Restoration (RTO):** The speed at which data can be restored, known as the Recovery Time Objective (RTO), is a critical metric in evaluating the effectiveness of a backup strategy. Different types of backups contribute to varying restoration speeds. Snapshots offer near-instantaneous recovery, while local copies provide a balance between speed and storage capacity. Archive copies, although secure and durable, may take longer to restore due to their offsite or offline nature.
- **Granular Restores vs. Large-Scale:** Not all data loss scenarios require a large-scale recovery. Granular restores, which involve retrieving specific files, folders, or even individual records, can be more targeted and efficient. This approach minimizes downtime by focusing on the essential elements, as opposed to restoring entire systems or databases. Evaluating the need for granular restores versus large-scale recoveries ensures a tailored and resource-efficient recovery process.

- **Testing & Validation of Restore Process:** Regular testing and validation of the restore process are paramount to guaranteeing its efficacy. Conducting simulated recovery scenarios, including both common and rare data loss situations, helps identify potential challenges and allows for refinements to the documented restore process. This proactive approach minimizes surprises during actual incidents and instills confidence in the organization's ability to recover data successfully.
- **Restore into Different Environments:** The ability to restore data into different environments is a testament to the flexibility and adaptability of a backup strategy. Whether migrating to new hardware, transitioning between on-premises and cloud environments, or deploying data for development and testing purposes, a robust restore capability ensures seamless operations across diverse IT landscapes.

Visibility & Analytics

Visibility and analytics are essential in data protection for identifying threats, assessing risks, and ensuring compliance with regulations. Visibility allows monitoring of data flow to detect anomalies, while analytics provide insights for proactive threat identification.

This information aids incident response, forensic investigations, and continuous improvement of data protection strategies. Both components are crucial for understanding, securing, and adapting to the evolving landscape of data security.

05

Disaster Recovery

Cyber resilience goes beyond merely preventing cyber threats; it involves anticipating and preparing for potential disruptions. Disaster Recovery (DR) specifically addresses the aftermath of a cyber incident, providing a structured approach to recover IT operations, minimize downtime, and mitigate the impact on business continuity.

By incorporating robust DR measures into a cyber-resilience strategy, organizations can enhance their ability to respond effectively to cyberthreats, ensuring a rapid and resilient recovery from adverse events.

Key components of an effective DR strategy include:

- **Risk Assessment:** Identifying potential risks and vulnerabilities to IT systems and data, including those related to cyberthreats, natural disasters, or human error.
- **Business Impact Analysis (BIA):** Assessing the potential impact of a disruptive event on critical business functions and determining the acceptable downtime for each.
- **Backup Systems:** Implementing regular and secure backups of critical data and systems to ensure their availability for recovery purposes.
- **Recovery Point Objective (RPO) and Recovery Time Objective (RTO):** Establishing RPO and RTO targets to define the maximum allowable data loss and the acceptable timeframe for systems to be restored.
- **Emergency Response:** Defining procedures for an immediate response to a disruptive event, including communication protocols, incident reporting, and activation of the DR plan.
- **Alternate Facilities:** Identifying and preparing alternate locations or facilities where operations can be temporarily shifted in the event of a physical site failure.
- **Data Replication:** Implementing mechanisms for real-time or near-real-time data replication to secondary sites, ensuring data consistency and availability.

- **Testing and Exercising:** Regularly testing and validating the DR plan through simulation exercises to ensure its effectiveness and identify areas for improvement.
- **Documentation:** Maintaining thorough documentation of the DR plan, including contact information, procedures, and key resources, to facilitate a swift and coordinated response.
- **Continuous Improvement:** Periodically reviewing and updating the DR plan to reflect changes in the IT environment, business operations, or emerging threats, ensuring ongoing relevance and effectiveness.
- **Training and Awareness:** Training staff on their roles and responsibilities during a disaster recovery scenario and promoting awareness of the DR plan throughout the organization.
- **Vendor and Partner Coordination:** Coordinating with third-party vendors and partners to ensure their alignment with the DR strategy and to leverage their support when needed.

By integrating these elements into a comprehensive DR plan, organizations can enhance their resilience to various disruptions, safeguard critical data, and minimize the impact on business continuity in the face of unforeseen events.

82% of organizations have an availability gap between how fast they can recover versus how fast they need applications to be recovered.

- [Veeam](#)

06

Incident Response

Effective incident response is a structured and coordinated approach to identifying, managing, and mitigating the impact of security incidents on an organization's IT systems and data. Key characteristics of effective incident response include:

- **Preparedness:** Establishing a well-defined incident response plan that includes clear roles and responsibilities, communication protocols, and procedures for reporting and documenting incidents.
- **Identification:** Promptly detecting and identifying security incidents, which may include unauthorized access, data breaches, malware infections, or other suspicious activities.
- **Containment:** Taking immediate action to contain the incident, preventing it from spreading further and minimizing the potential damage or impact on systems and data.
- **Eradication:** Identifying and eliminating the root cause of the incident to prevent its recurrence. This may involve removing malware, closing vulnerabilities, or implementing corrective measures.
- **Recovery:** Restoring affected systems and data to a secure and operational state. This includes validating the integrity of restored systems to ensure they are free from vulnerabilities.
- **Communication:** Maintaining clear and timely communication throughout the incident response process. This involves keeping stakeholders informed about the incident, its impact, and the progress of containment and recovery efforts.
- **Coordination:** Coordinating efforts among different teams, including IT, security, legal, and communication teams, to ensure a cohesive and well-managed response to the incident.
- **Documentation:** Thoroughly documenting all aspects of the incident response process, including actions taken, findings, and lessons learned. This documentation is valuable for post-incident analysis and for refining incident response procedures.

- **Continuous Improvement:** Regularly reviewing and updating incident response plans and procedures based on lessons learned from each incident. This ensures that the organization is continually improving its ability to respond effectively to evolving cyber threats.
- **Legal and Regulatory Compliance:** Adhering to legal and regulatory requirements related to incident reporting and disclosure. Effective incident response includes understanding and fulfilling any legal obligations associated with a security incident.
- **Training and Awareness:** Providing ongoing training to incident response teams and raising awareness among employees about security best practices. This ensures that individuals are well-prepared to recognize and report potential incidents.

A well-executed incident response strategy enables organizations to minimize the impact of security incidents and recover quickly, safeguarding their operations and reputation.



07

Conclusion

In the face of vigilant attackers seeking opportunities to exploit systems, companies must transition their security approach from a reactive stance to one of anticipation. Cyber resilience, as a proactive strategy, anticipates cyber incidents and prioritizes planning and training to ensure seamless business continuity.


It's crucial to recognize that cyber resilience is not a one-time initiative; rather, it demands continuous effort, sustained attention, and ongoing investment. While the commitment may be persistent, the dividends include enhanced protection of digital assets and the preservation of your reputation, trust, and credibility with stakeholders.

Are you interested in learning more about building a cyber-resilient architecture in your organization? Check out the [ANM Cyber-Resilient Architecture Workshop](#).





anm^o

 (866) 527-8822

 info@anm.com

 anm.com